

REMARKS / ARGUMENTS

In response to the Office Action mailed November 28, 2005 ("Office Action"), Applicant respectfully requests that the Office enter the amendments set forth above and consider the following remarks. By this amendment, Applicant amends claims 7, 28, 35, and 42. After entry of this paper, claims 7-13 and 28-47 will remain pending in this application.

In the Office Action, the Examiner: (i) objected to an informality in the specification; (ii) rejected claim 7 and the "intervening claims" under 35 U.S.C. § 112; and (iii) rejected claims 7-13 and 28-47 under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,047,242 to Benson ("Benson") in view of U.S. Patent No. 6,009,543 to Shavit ("Shavit").

Objection to the Specification

Applicant thanks the Examiner for noting the inadvertent error in the disclosure. Applicant has amended the drawings and specification accordingly; namely, the trusted element in Figures 15 and 21 is now labeled with reference number 109 rather than reference number 108, which had already been used in a previous Figure. Applicant respectfully submits that the objection has thus been overcome.

Rejection of Claim 7 and Intervening Claims under 35 U.S.C. § 112

Claim 7 and certain other claims (Applicant is unsure precisely which) were rejected under 35 U.S.C. § 112 as allegedly failing to comply with the written description requirement. Applicant respectfully disagrees with the Examiner's rejection, and points out that representative support for the claim elements identified by the Examiner can be found in the drawings at, e.g., Figure 15 (showing an application running in an insecure execution space), and in the specification at, e.g., page 30, lines 11 and 18-24; and page 31, lines 13-22 (describing an application running in an insecure execution space, and the issuance of challenges thereto), and at, e.g., page 31, line 3 through page 32, line 6; page 33, lines 3-12; and page 37, line 27 through page 38, line 2 (describing the use of a credential to detect

modification of an application). Nevertheless, in the interest of expediting prosecution of this application, Applicant has amended claim 7 in a manner that is believed to ameliorate Examiner's concerns.

Rejection of Claims 7-13 and 28-47 under 35 U.S.C. § 103(a)

Claims 7-13 and 28-47 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Benson in view of Shavit. Applicant respectfully submits that the pending claims are allowable over Benson in view of Shavit for at least the reasons set forth below.

Claim 7 recites a trusted element for use with a computer system that includes an insecure execution space for executing an application. The trusted element selects a portion of the application that includes at least some code, and issues a challenge that requests a response from the insecure execution space, the response providing a computation of at least one value based on the selected portion of the application.

Applicant respectfully submits that neither Benson nor Shavit teaches or suggests a trusted element as recited in Applicant's claim 7. With respect to Benson, unlike claim 7, in which a challenge is generated based on a predetermined portion of an application that includes at least some of the application's actual code, Benson describes a fundamentally different challenge/response mechanism that is based on proof of possession of hidden keying material. This keying material is not a portion of the application's **code** as recited in claim 7. In contrast, the trusted element recited in Applicant's claim 7 makes use of portions of the application's **code**, thus providing a mechanism for ensuring that the application has not been tampered with.

With respect to Shavit, Applicant respectfully notes that the Examiner appears to have applied Shavit to claim 8, not claim 7 (see Office Action at pages 6 and 7, alleging that Shavit teaches *inter alia* the random selection of one of the plural predetermined portions). In any event, Applicant respectfully submits that Shavit, like Benson, fails to teach or suggest at least "a challenge generator that selects, based at least in part on the credential, at least one predetermined portion of the

application, the predetermined portion of the application including at least some code, and issues a challenge requesting a response from the insecure arrangement, the response providing a computation of at least one value based on the selected predetermined portion of the application” as recited by Applicant’s claim 7. Indeed, the cited portions of Shavit do not teach or suggest a challenge/response mechanism as recited in Applicant’s claim 7, in which the challenge and the response involve the selection of a portion of an application and the computation of at least one value based on the selected portion. Instead, as understood, the cited portions of Shavit relate to a very different context, in which an application is split into parts. As such Applicant’s respectfully submit that not only does the combination of Benson and Shavit fail to teach each of the elements of Applicant’s claim 7, but it would also not have been obvious to combine Shavit with Benson.

Finally, although the Examiner has indicated at pages 2 and 3 of the Office Action that Herzberg may also be relevant to the pending claims, Applicant notes that the Examiner has not included Herzberg in the actual rejection under 35 U.S.C. § 103(a) that appears at pages 5 through 9 of the Office Action. In any event, Applicant respectfully submits that Herzberg fails to anticipate or render obvious Applicant’s claim 7 (or any of the other pending claims).

Claims 8-13 are dependent from claim 7, and are thus allowable for at least the reasons set forth above in connection with claim 7.

Claims 28, 35, and 42 each recite a challenge requesting an application or agent to provide one or more cryptographic hashes of one or more portions of the application. Applicant respectfully submits that neither Benson nor Shavit teaches this limitation. Although the Examiner has apparently conceded that Benson fails to teach this limitation, it appears that the Examiner believes that Shavit does include such a teaching. However, Applicant respectfully submits that, to the extent Shavit teaches the use of “hashing”, it is not in the manner, nor for the purpose, recited in Applicant’s claims. In particular, it appears that Shavit uses the term “hashing” to simply refer to changing the order of fragments in a program, not to the use of cryptographic hashing as described in Applicant’s disclosure and recited in Applicant’s claims. Finally, Applicant respectfully submits that, for at least the reasons previously set forth above, it

would not have been obvious to combine Benson with Shavit.

Claims 29-34 are dependent from claim 28, and are thus allowable for at least the reasons set forth above in connection with claim 28. Claims 36-41 are dependent from claim 35, and are thus allowable for at least the reasons set forth above in connection with claim 35. Claims 43-47 are dependent from claim 42, and are thus allowable for at least the reasons set forth above in connection with claim 42.

Amendment of Claims 28, 35 and 42

Claims 28, 35 and 42 have been amended to correct minor typographical errors. These amendments have been made to improve the readability of the claims, not for purposes of patentability. No new matter has been added.

CONCLUSION


Applicant submits that the pending claims are in allowable form, and respectfully requests their timely allowance.

Please grant any extensions of time required to enter this response and charge any additional required fees to our Deposit Account No. 06-0916.

Respectfully submitted,

FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER, L.L.P.

Dated: May 30, 2006

By: 
Andrew B. Schwaab
Reg. No. 38,611

**Attachments: Tab A - 2 Replacement Sheets, Figs. 15 and 21
Tab B - 2 Annotated Sheets - Figs. 15 and 21, showing changes**

Finnegan, Henderson, Farabow
Garrett & Dunner, L.L.P.
901 New York Ave., N.W.
Washington, D.C. 20001
Attorney direct (650) 849-6643